Amendments to the Claims:

1. (Currently amended) A distributed system for monitoring a communications network and for detecting, tracing and retaliating to an unauthorized communications access attempt into the monitored communications network, the system comprising:

one or more distributed hierarchical monitoring systems; and

one or more alarm signals that represent an unauthorized communications access attempt into one or more localized portions of the monitored communications network~~,~~;

wherein the one or more distributed hierarchical monitoring systems analyze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, including sending a mechanism for verifying the presence of an attack and for immediately determining a source of the unauthorized communications access attempt ~~in a response to the unauthorized communications access attempt;~~

wherein the verifying mechanism sends a determining mechanism that determines if the source of the unauthorized access attempt is hostile;

wherein the determining mechanism includes an identified packet concealed in the response, and the one or more distributed hierarchical monitoring systems detect passage of the identified packet;

wherein the packet is identified by a flag, and the one or more distributed hierarchical monitoring systems comprise conduit hosts and participating nodes forming a cooperative reporting system to detect passage of the flag and record information related to the flag and associated data, thereby revealing the source of the unauthorized communications access attempt regardless of a number of intermediate steps used to avoid detection by the source of the unauthorized communication access attempt;

wherein the identified packet triggers the reporting and showing of a path to the source of the unauthorized communication access attempt;

wherein subject to applicable laws an immediate counter-attack is launched, anytime after commencement of the unauthorized communication access attempt;

wherein the counter-attack comprises a concealed program embedded with additional levels of verification to ensure the hostile intent and identity of the source of the unauthorized

communication access attempt in addition to destructive means for destroying the files and/or operating system of a computer of the source of the unauthorized communication access attempt;

wherein the additional levels of verification of hostile intent and identity of the source of the unauthorized communication access attempt are based on an historical profile, other previous attempts by the source of the unauthorized communication access attempt or communication with other monitoring centers to determine whether other targets have been attacked with same or similar unauthorized access requests; and

wherein upon verification of hostile intent and identity of the source of the unauthorized communication access attempt, the identification of the source of the unauthorized communication access attempt is secretly forwarded to a target station or monitoring center and via the counter-attack files and/or operating system of the computer of the source of the unauthorized communication access attempt are destroyed.

2. (Previously presented) The system of claim 1, further comprising a monitoring device that monitors information on one or more monitored communications networks.

3. (Previously presented) The system of claim 1, further comprising an intrusion analysis system that receives the one or more alarm signals and at least one of determines the origin of the unauthorized communications access attempt, logs communications and evaluates the threat of the unauthorized communications access attempt.

4. (Previously presented) The system of claim 1, further comprising an intrusion interaction system that is capable of communicating with the origin of the unauthorized communications access attempt.

5. (Previously presented) The system of claim 1, further comprising an escalation determination system that, based on an evaluation of the unauthorized communications access attempt and a comparison to one or more other unauthorized communications access attempts, forwards information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

6. (Previously presented) The system of claim 1, wherein the one or more alarm signals is generated by one or more recipients of the unauthorized communications access attempt.

7. (Previously presented) The system of claim 1, further comprising a response system that communicates information regarding the unauthorized communications access attempt to one or more of a monitored site and a law enforcement agency.

8. (Currently amended) A method for monitoring a communications network and for detecting, tracing and retaliating to an unauthorized communications access attempt into the monitored communications network, the method comprising:

monitoring one or more portions of the monitored communications network through one or more distributed hierarchical monitoring systems; and

receiving one or more alarm signals that represent an unauthorized communications access attempt into one or more localized portions of the monitored communications network,

wherein the one or more distributed hierarchical monitoring systems analyze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, including sending a mechanism for verifying the presence of an attack and for immediately determining a source of the unauthorized communications access attempt ~~in a response to the unauthorized communications access attempt;~~

wherein the verifying mechanism sends a determining mechanism that determines if the source of the unauthorized access attempt is hostile;

wherein the determining mechanism includes an identified packet concealed in the response, and the one or more distributed hierarchical monitoring systems detect passage of the identified packet;

wherein the packet is identified by a flag, and the one or more distributed hierarchical monitoring systems comprise conduit hosts and participating nodes forming a cooperative reporting system to detect passage of the flag and record information related to the flag and

associated data, thereby revealing the source of the unauthorized communications access attempt regardless of a number of intermediate steps used to avoid detection by the source of the unauthorized communication access attempt;

wherein the identified packet triggers the reporting and showing of a path to the source of the unauthorized communication access attempt;

wherein subject to applicable laws an immediate counter-attack is launched, anytime after commencement of the unauthorized communication access attempt;

wherein the counter-attack comprises a concealed program embedded with additional levels of verification to ensure the hostile intent and identity of the source of the unauthorized communication access attempt in addition to destructive means for destroying the files and/or operating system of a computer of the source of the unauthorized communication access attempt;

wherein the additional levels of verification of hostile intent and identity of the source of the unauthorized communication access attempt are based on an historical profile, other previous attempts by the source of the unauthorized communication access attempt or communication with other monitoring centers to determine whether other targets have been attacked with same or similar unauthorized access requests; and

wherein upon verification of hostile intent and identity of the source of the unauthorized communication access attempt, the identification of the source of the unauthorized communication access attempt is secretly forwarded to a target station or monitoring center and via the counter-attack files and/or operating system of the computer of the source of the unauthorized communication access attempt are destroyed.

9. (Previously presented) The method of claim 8, further comprising monitoring information relating to one or more geographic or organizational portions of the monitored communications networks.

10. (Previously presented) The method of claim 8, further comprising receiving the one or more alarm signals and at least one of determining the origin of the unauthorized communications access attempt, logging communications and evaluating the threat of the unauthorized communications access attempt.

11. (Previously presented) The method of claim 10, wherein the logging can be restricted based on an analysis of the unauthorized communications access attempt.

12. (Previously presented) The method of claim 8, further comprising communicating with the origin of the unauthorized communications access attempt.

13. (Previously presented) The method of claim 8, further comprising forwarding, based on an evaluation of the unauthorized communications access attempt and a comparison to one or more other unauthorized communications access attempts, information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

14. (Previously presented) The method of claim 8, wherein the one or more alarm signals is generated by one or more recipients of the unauthorized communications access attempt.

15. (Previously presented) The method of claim 8, further comprising communicating information regarding the unauthorized communications access attempt to one or more of a monitored site and a law enforcement agency.

16. (Previously presented) The system of claim 1, wherein the one or more distributed hierarchical monitoring systems forward information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

17-20. (Cancelled)

21. (Currently amended) The system of ~~claim 20~~ claim 1, wherein the concealed program is concealed in an HTML page sent as part of the response.

22. (Previously presented) The method of claim 8, wherein the one or more distributed hierarchical monitoring systems forward information regarding the unauthorized communications access attempt to one or more of the one or more distributed hierarchical monitoring systems.

23-26. (Cancelled)

27. (Currently amended) The method of ~~claim 26~~ claim 8, wherein the concealed program is concealed in an HTML page sent as part of the response.

28. (Previously presented) The method of claim 8, further comprising implementing said method via a computer program product including one or more computer-readable instructions configured to cause one or more computer processors to perform the steps of the method.

29. (Previously presented) The system of claim 2, wherein the monitored information relates to one or more geographic or organizational portions of the monitored communications networks.

30. (New) A distributed system for monitoring a communications network and for detecting, tracing and responding to an unauthorized communications access attempt into the monitored communications network, the system comprising:

one or more distributed hierarchical monitoring systems; and

one or more alarm signals that represent an unauthorized communications access attempt into one or more localized portions of the monitored communications network;

wherein the one or more distributed hierarchical monitoring systems analyze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, including sending a mechanism for verifying the presence of an attack and for immediately determining a source of the unauthorized communications access attempt ;

wherein the verifying mechanism sends a determining mechanism that determines if the source of the unauthorized access attempt is hostile;

wherein the determining mechanism includes an identified packet concealed in the response, and the one or more distributed hierarchical monitoring systems detect passage of the identified packet;

wherein the packet is identified by a flag, and the one or more distributed hierarchical monitoring systems comprise conduit hosts and participating nodes forming a cooperative reporting system to detect passage of the flag and record information related to the flag and associated data, thereby revealing the source of the unauthorized communications access attempt regardless of a number of intermediate steps used to avoid detection by the source of the unauthorized communication access attempt;

wherein the identified packet triggers the reporting and showing of a path to the source of the unauthorized communication access attempt;

wherein an immediate response is launched, anytime after commencement of the unauthorized communication access attempt;

wherein the response comprises a concealed program embedded with additional levels of verification to ensure the hostile intent and identity of the source of the unauthorized communication access attempt;

wherein the additional levels of verification of hostile intent and identity of the source of the unauthorized communication access attempt are based on an historical profile, other previous attempts by the source of the unauthorized communication access attempt or communication with other monitoring centers to determine whether other targets have been attacked with same or similar unauthorized access requests;

wherein upon verification of hostile intent and identity of the source of the unauthorized communication access attempt, the identification of the source of the unauthorized communication access attempt is secretly forwarded to a target station or monitoring center; and

wherein one or more distributed hierarchical monitoring systems include first through third level monitoring systems, with the first level monitoring system configured to monitor a predetermined geographical area, an organizational structure or defined cyber boundaries, and refer the unauthorized access attempt to an appropriate second level monitoring system,

with the second level monitoring system configured to receive the referral from the first level monitoring system and make a decision on a possible response based a nature of the unauthorized access attempt, and receive and analyze cumulative information on unauthorized access attempts from underlying first level monitoring systems, and with the third level monitoring system configured to collect and analyze information from the second level monitoring system, and monitor an overall security condition of the monitored communications network.